THE UNIVERSITY OF WINNIPEG

POLICY TITLE: **Acceptable Use of Information Technology Policy**

EFFECTIVE DATE: **September 25, 2017**

APPROVAL BODY: **University Administration**

POLICY PURPOSE

The purpose of this Policy is to establish clear rules and regulations pertaining to the behaviour of individuals engaged in activities using University of Winnipeg Information Technology (IT) Resources.

LEGAL AUTHORITY

Not Applicable

APPLICABILITY

This Policy applies to:

a) all Users; and

b) all activities conducted using any IT Resource including data input or output, data storage, computation, or as a digital communications resource.

RESPONSIBILITY

The Vice-President, Finance and Administration, on behalf of the University, is responsible for the development and review of this Policy. The Chief Information Officer is responsible for the administration of this Policy.

KEY DEFINITIONS

The following definitions apply to terms as they are used in this Policy:

- **"CIO"** - the most senior employee of the University charged with oversight and stewardship of the University's IT Resources.
- **"Device"** - any computing or data storage equipment, whether mobile, stationary including, but not limited to:
  - desktop computers;
  - laptops (a mobile computer small enough to fit on a user's lap);
  - mobile computing devices (computing devices smaller than laptops, such as smartphones, tablet computers); and
  - mobile storage devices / media (portable devices used to store electronic information, such as USB sticks, portable drives, memory cards, CDs, DVDs).

- **"IT Resource"** - Information Technology services, Devices, and facilities that are owned, leased, administered by or provided by the University of Winnipeg including, but not limited to:
  - computers and computer facilities;
  - computing hardware and equipment;
  - mobile computing Devices;
  - electronic storage Devices;
  - email systems;
  - telephone and other voice systems;
  - software; and
  - any hardware, software, or network facility used to capture, store, retrieve, output, transfer, communicate, or disseminate information through the use of information technology.

- **"University Business"** means activities in support of the academic, research and service mandates of the University. For employees this includes all activities performed as part of their employment duties.

- **"User"** - individuals who have been granted the right to access the University's IT Resources including, but not limited to:
  - Faculty, staff and all employees of the University;
  - academics visiting or conducting research at the University;
  - students enrolled at the University;
  - parties affiliated with the University;
  - guests; and
  - authorized third-parties (e.g., contractors, suppliers, tenants, etc.).

- **"User Identity"** - anything that can be used to identify a User, such as a logon account, password, biometric characteristic, token, IP address, card, etc.

POLICY ELEMENTS

Principles

a) IT Resources provide critical support for the teaching, research and service missions of the University. The loss of these resources could threaten the University's ability to deliver on its mission. Appropriate and reasonable constraints on the use of IT Resources are necessary to ensure these resources are available to support the University's mission.

b) The University of Winnipeg provides Users with IT Resources to support the academic, research and service mandates as well as the administration of the University on the premise that all uses shall be complementary to the objectives of those mandates.

c) User conduct that negatively affects the University's learning, research, and administrative support environment, undermines Users in performing their responsibilities, or negatively impacts the reputation of the University shall be construed as a breach of this Policy.

d) Users will use IT Resources in compliance with applicable laws, university policies, and in a manner that protects the University's assets from harm.
e) This Policy extends to use of privately-owned Devices that interact in any manner with University IT Resources or are used for University-related purposes.

Acknowledgement of Compliance

All Users of University IT Resources shall be required to acknowledge that they have familiarized themselves with the provisions of this Policy and agree to be bound by it. Any User failing to do so shall be denied access to the University's IT Resources.

Responsibilities of Parties

1. ***CIO*** – This individual is the Custodian of the University's IT Resources responsible for managing, administering, and safekeeping such IT Resources.
2. ***IT Resource Users*** **–** Use of the University's IT Resources also carries with it certain responsibilities. All Users of the University's IT Resources are required to:
    a) use IT Resources only for University Business, although incidental personal use is permissible provided that such use does not interfere with the User's job performance or student experience, does not increase operational costs for IT Resources, and is not an Unacceptable Use of IT Resources as described below
    b) keep secure the User Identity provided to them since they are responsible for all activity generated using that Identity;
    c) use only the User Identity they have been authorized to use, comply with all restrictions that apply to that User Identity, and never impersonate another identity;
    d) comply with all IT security measures adopted by the University;
    e) comply with all laws, including those related to privacy of information, software licensing, intellectual property, and trademarks;
    f) obtain permission before accessing, copying, modifying or deleting another person's personal data files or information;
    g) understand and respect the policies governing the use of other entities' IT Resources accessed in the course of University-related activity, or by using University IT Resources;
    h) comply with all relevant University Human Research Ethics Board (UHREB) policies and the Tri-Council Policy Statement (TCPS2) guidelines in research activities involving computers; and
    i) immediately report any suspected unacceptable use of IT Resources to the Technology Service Desk or one of these respective parties:
        - in the case of employees, their immediate supervisor;
        - in the case of students, the Office of the Registrar;
        - in matters related to academic research, the Vice-President, Research and Innovation; and
        - in the case of third parties, the CIO.

Unacceptable Use of IT Resources

The following list is intended to provide guidance in determining whether an activity or behaviour would cause the User to be in breach of this Policy:

a) distributing content or carrying on activities prohibited by the laws of Canada, a province, or international convention;

b) contravening the Freedom of Information and Protection of Privacy Act (FIPPA), the Personal Health Information Act (PHIA), the Personal Information Protection and Electronic Documents Act (PIPEDA), and similar legislation;

c) downloading or disseminating licensed software, copyrighted materials, or derivative works in breach of applicable laws;

d) any activity that results in breach of University Human Research Ethics Board (UHREB) policies and the Tri-Council Policy Statement (TCPS2) guidelines in research activities involving computers;

e) attempting to gain access to another person's User Identity;

f) sending messages that are under false pretence, fraudulent, harassing, threatening, obscene, or perpetrating scams and hoaxes;

g) mass dissemination of messages or e-mails not approved by University Administration;

h) using IT Resources for personal gain not related to the University Business, including transmitting commercial advertisements, solicitations, or promotions not approved by University Administration;

i) engaging in any uses that result in the loss of another User's information without authorization

j) attempting to sabotage or in any way circumvent security measures of the University or other entities' IT Resources;

k) depriving others of access to the University's or other entities' IT Resources;

l) any activity that results in disruption, degradation, or interference with the normal operation of the University's or other entities' IT Resources or services; and

m) any activity that results in breach of other related policies as denoted below in the 'Related Policies' section.

The above list is not intended to be exhaustive. Any User who may be in doubt as to the acceptability of a specific use of IT Resources should seek guidance from the following parties:

a) in the case of employees, their immediate supervisor;

b) in the case of students, the Office of the Registrar;

c) in matters related to academic research, the Vice-President, Research and Innovation; and

d) in the case of third parties, the CIO.

Exemptions from Policy

There may be situations where legitimate University Business may cause the User to be out of compliance with this Policy. The User must seek an exemption for such undertaking (prior, where possible) by making a formal exemption request to the Vice-President, Finance and Administration stating:

a) the reasons for the exemption;

b) the IT Resources that will be used; and

c) the duration of the exemption requested.

Upon receiving such approval, and if it is practical to do so, any technical controls that protect the IT Resource will be lifted for the exemption period.

Consequences of Unauthorized or Unacceptable Use

The University may investigate the use of IT Resources using all necessary means including, but not limited to, reviewing the contents of data stored on or transmitted using University IT Resources. Investigations shall be conducted in accordance with applicable legislation, University policies, and collective agreements. Based on the findings of such investigation, the Vice-President, Finance and Administration in consultation with the CIO and other appropriate senior administrators shall determine the action needed to:

a) end the unacceptable activity or conduct;

b) protect the University's IT environment; and

c) protect the University from any adverse consequences including potential liability, or damage to its reputation or assets.

The University shall comply with any subpoena, warrant, or other court order requiring the University to provide law enforcement authorities with access to IT Resources and usage records for a User, User Identity, or IT Resource.

Violators will have their User Identity disabled and will be subject to disciplinary procedures set out in:

a) the Student Non-Academic Misconduct Policy;

b) University of Winnipeg Collective Agreements; or

c) such other Policies, procedures, or protocols as may apply.

In cases of financial loss to the University, the University may seek restitution. In severe cases, criminal prosecution could result.

ASSOCIATED PROCEDURES

- Not Applicable

RELATED POLICIES

- Conflict of Interest Policy
- Copyright Policy
- Discipline & Dismissal of Support Staff Excluded from Bargaining Units
- Privacy Policy
- Respectful Working and Learning Environment Policy
- Responsible Conduct of Research and Scholarship Policy
- Student Academic Misconduct Policy
- Student Non-Academic Conduct and Discipline Policy

RELEVANT DATES

Originally Issued: **September 1, 2004**

Revised: **September 5, 2017**

Effective: **September 25, 2017**

Scheduled Review: **September 25, 2022**